Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. *(Currently Amended)* A document security system for restricting access to secured documents, the system comprising:

a processor;

a policy system configured to enable the processor to store at least one process-driven security policy on a computer readable storage medium, wherein the process-driven security policy includes a plurality of different states and transition rules, [[and]] wherein each of the different states is associated with one or more access restrictions, [[and]] wherein at least one of the different states has distinct access restrictions for secured documents which reside in that state, and wherein the transition rules specify circumstances under which a secured document is to transition from one state to another, wherein the secured document includes at least a security information portion and an encrypted data portion, the security information portion including at least an encrypted file key, [[and]] wherein the circumstances include the occurrence of internal and external events, wherein the external events originate from outside the policy system and wherein in response to detecting a transition from a previous state of the process-driven security policy for the secured document to a current state, the secured document is modified by decrypting the file key and then re-encrypting the file key, whereby the file key is encrypted differently for the current state than the previous state;

wherein the policy system is configured to enable the processor to provide a reference to the process-driven security policy to a client computer, the reference referring to the process-driven security policy and an accessor user list resident on the policy system; and

an access manager configured to enable the processor to access the process-driven security policy and determine whether a requestor is permitted to access a secured document based on the policy state associated therewith at the time access is requested, the requestor being listed in the accessor user list, and the corresponding one or more access restrictions thereof for the process-driven security policy.

2. *(Previously presented)* The document security system as recited in claim 1, wherein the one or more access restrictions for the secured document are automatically changed in response to detecting a change in the state of the process-driven security policy for the secured document.

3. *(Previously presented)* The document security system as recited in claim 1, wherein events cause the state of the process-driven security policy for the secured document to automatically transition from one state to another.

4. *(Previously presented)* The document security system as recited in claim 3, wherein the internal events originate from the document security system and wherein external events originate from outside the document security system.

5. *(Previously Presented)* The document security system as recited in claim 4, wherein at least one of the external events originates from a document management system.

6. *(Previously presented)* The document security system as recited in claim 1, wherein one or more of the corresponding one or more access restrictions for access to the secured document remain intact when the state of the process-driven security policy for the secured document changes.

7. *(Previously presented)* The document security system as recited in claim 1, wherein events cause the state of the process-driven security policy to automatically transition from one state to another, wherein the process-driven security policy includes at least a first state, a second state, and a third state, and wherein a first event causes transition from the first state to the second state, and a second event causes transition from the second state to a third state.

8. *(Previously presented)* The document security system as recited in claim 1, wherein events cause the state of the process-driven security policy to automatically transition from one state to another, wherein the process-driven security policy includes at least a first state and a second state, and wherein a first event causes transition from the first state to the second state.

9. *(Previously presented)* The document security system as recited in claim 1, wherein the external events originate from a second document security system.

10. *(Previously presented)* The document security system as recited in claim 9, wherein the transition rules are written in XML.

11. *(Previously presented)* The document security system as recited in claim 1, wherein events cause the state of the process-driven security policy for the secured document to transition from a previous state to a current state, and wherein the secured document is modified in response to detecting a transition from the previous state of the process-driven security policy for the secured document to the current state.

12. *(Currently Amended)* The document security system as recited in claim 11, wherein the ~~secured document includes at least a security information portion and an encrypted data portion, the security information portion including at least an encrypted key, and the~~ file key ~~being encrypted~~ is decrypted in order to decrypt the encrypted data portion~~, and wherein in response to detecting a transition from the previous state of the process-driven security policy for the secured document to the current state, the secured document is modified by decrypting the encrypted key and then re-encrypting the key, whereby the key is encrypted differently for the current state than the previous state~~.

13. *(Previously presented)* The document security system as recited in claim 11, wherein, in response to determining, by the access manager, that access to a secured document is permitted by a requestor, access to the secured document is available at a client machine associated with the requestor.

14. *(Currently Amended)* A method for transitioning at least one secured document through a security-policy state machine having a plurality of different states, each of the plurality of different states having distinct access restrictions for secured documents which reside in that state, the method comprising:

receiving an event, wherein the event is one of a group of internal and external events, wherein the external events originate from outside the security-policy state machine;

determining whether the event causes a state transition for the at least one secured document from a former state to a subsequent different state of the security-policy state machine;

automatically transitioning from the former state to the subsequent different state of the security-policy state machine in response to determining that the event causes the state transition, wherein the at least one secured document includes at least a security information portion and an encrypted data portion, the security information portion including at least an encrypted file key, and wherein the transitioning comprises modifying the at least one secured document by decrypting the encrypted file key and then re-encrypting the file key, whereby the file key is encrypted differently for the current state than the former state; and

providing a reference to the security-policy state machine to a client computer, the reference referring to a current state of the security-policy state machine and an accessor user list resident in the security-policy state machine.

15. *(Previously presented)* The method as recited in claim 14, wherein the security-policy state machine implements a process-driven security policy, and wherein each state of the security-policy state machine has different access restrictions.

16. *(Previously presented)* The method as recited in claim 14, wherein each of the states of the security-policy state machine have different access policies.

17. *(Previously presented)* The method as recited in claim 16, wherein the security-policy state machine is provided as part of a document security system, and wherein the different access policies of the security-policy state machine are enforced by the document security system.

18. *(Previously presented)* The method as recited in claim 14, wherein the transitioning comprises modifying the secured document to reflect the subsequent state of the security-policy state machine.

19. *(Currently Amended)* The method as recited in claim 14, wherein the transitioning further comprises:

retrieving [[an]] <u>the</u> encrypted file key from the secured document;

decrypting the encrypted file key to yield [[a]] the file key;

subsequently encrypting the file key in accordance with the subsequent state of the security-policy state machine; and

storing the secured document, the secured document including at least an encrypted data portion and the subsequently encrypted file key.

20. *(Currently Amended)* The method as recited in claim 14, wherein the transitioning further comprises:

retrieving [[an]] the encrypted file key from the secured document;

obtaining a private state key associated with the former state of the security-policy state machine;

decrypting the encrypted file key using the private file key;

obtaining a public state key associated with the subsequent state of the security-policy state machine;

subsequently encrypting the file key in accordance with the public state key; and

storing the secured document, the secured document including at least an encrypted data portion and the subsequently encrypted file key.

21. *(Currently Amended)* A method for imposing access restrictions on electronic documents, the method comprising:

providing at least one process-driven security policy at a server computer, wherein the process-driven security policy is associated with a plurality of

different states, and wherein each of the different states has distinct access restrictions for secured documents which reside in that state;

providing a reference to the process-driven security policy to a client computer, the reference referring to the process-driven security policy and an accessor user list resident on the server computer;

associating the reference to an electronic document;

transitioning the process-driven security policy from one state to a current state in response to the occurrence of an event, wherein the event is one of a group of internal and external events, wherein the external events are external to the server computer, wherein the electronic document includes at least a security information portion and an encrypted data portion, the security information portion including at least an encrypted file key, and wherein the transitioning comprises modifying the electronic document by decrypting the encrypted file key and then re-encrypting the file key, whereby the file key is encrypted differently for the current state than the former state; and

subsequently determining at the server computer whether a requestor is permitted to access the electronic document, the access being based on a current state of the process-driven security policy and the requestor being listed in the accessor user list, the current state being informed to the server computer by sending the reference to the server computer.

22. *(Previously Presented)* The method as recited in claim 21, wherein the external events originate from a system external to the server computer.

23. *(Previously presented)* The method as recited in claim 22, wherein the transitioning is performed at the server computer.

24. *(Previously presented)* The method as recited in claim 21, wherein the associating associates the reference to a group of documents.

25. *(Previously presented)* The method as recited in claim 21, wherein the method pertains to a group of electronic documents, and wherein all of the electronic documents of the group are always in the same state of the process-driven security policy.

26. *(Previously presented)* The method as recited in claim 21, wherein the determining comprises evaluating the process-driven security policy of an electronic document at the server computer based on at least the security policy restrictions for the current state of the process-driven security policy for the electronic document.

27. *(Currently Amended)* A non-transitory computer readable storage medium having instructions stored thereon, the instructions comprising:

instructions to detect an occurrence of an event, wherein the event is one of a group of internal and external events;

instructions to determine whether the event causes a state transition for at least one secured document from a former state to a subsequent different state of

a security-policy state machine having a plurality of different states, each of the plurality of different states having distinct access restrictions for secured documents which reside in that state; and

instructions to automatically transition from the former state to the subsequent different state of the security-policy state machine upon determining that the event causes the state transition, wherein the external events originate from outside the security-policy state machine, and wherein the at least one secured document includes at least a security information portion and an encrypted data portion, the security information portion including at least an encrypted file key, and wherein the transitioning comprises modifying the at least one secured document by decrypting the encrypted file key and then re-encrypting the file key, whereby the file key is encrypted differently for the current state than the former state; and

instructions to provide a reference to the process-driven security policy to a client machine, wherein the reference refers to the process-driven security policy and an accessor user list resident in the security-policy state machine.

28. *(Currently Amended)* A non-transitory computer readable storage medium having instructions stored thereon, the instructions comprising:

instructions to provide at least one process-driven security policy at a server machine, wherein the process-driven security policy has a plurality of different states and transition rules associated therewith, [[and]] wherein each of the different states has distinct access restrictions for secured documents which

reside in that state, [[and]] wherein the transition rules specify circumstances under which an electronic document is to transition from one state to another, [[and]] wherein the circumstances include the occurrence of internal and external events, wherein the external events originate from outside the server machine, and wherein the at least one secured document includes at least a security information portion and an encrypted data portion, the security information portion including at least an encrypted file key, and wherein the transitioning comprises modifying the at least one secured document by decrypting the encrypted file key and then re-encrypting the file key, whereby the file key is encrypted differently for the current state than the former state;

instructions to provide a reference to the process-driven security policy to a client machine, wherein the reference refers to the process-driven security policy and an accessor user list resident on the server machine;

instructions to associate the reference to an electronic document;

instructions to transform the process-driven security policy from one state to a current state; and

instructions to determine at the server computer whether a requestor is permitted to access the electronic document, wherein the access is based on a current state of the process-driven security policy and the requestor being listed in the accessor user list, and wherein the current state is informed to the server computer by sending the reference to the server computer.